Methodology for balancing privacy and security

Gayrel, Claire; Poullet, Yves

Published in:
Circulation internationale de l'information et sécurité

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

METHODOLOGY FOR BALANCING PRIVACY AND SECURITY: THE INCREASING ROLE OF IMPACT ASSESSMENTS IN THE EU. BENEFITS AND RISKS

Claire GAYREL* et Yves POULLET**

* Chercheure au Centre de Recherche Information, Droit et Société (CRID)

** Recteur de l'Université de Namur

The adoption by the Office of the Privacy Commissioner of Canada of a reference document proposing a guide for a trust-inspiring balancing of privacy and security[1] constitutes an interesting methodological step to the privacy v. security debates occurring in Western democratic countries in the post 9/11 era. From "making the case" to "setting the stage", "running the program" and "calibrating the system", this document intends to provide a guiding tool to public security and national safety stakeholders when they are envisaging the implementation of surveillance measures. The purpose of this paper is to look at the European Union's developing practices as regards the methodology used for ensuring the balance between privacy and security. Though no specific comparable document exists in the European Union, the process described by the reference document (conception of the envisaged measure and analysis of its compliance with the *Oakes Test*)[2] is encapsulated under the general governance objectives of the EU in the matter of regulation. We will start by tracing back, in brief, the governance strategy of the EU, paying particular attention to the development and generalisation of impact assessments studies at the pre-legislative stage under the "better regulation" strategy and progressively increasing concern for human rights assessment (I). We will then focus on the examples in which a balancing of privacy and security has been dealt with in this framework, basing our comments on the three interrelated criteria for the validity of a norm: legitimacy, effectiveness and legality (II). Finally, we will see that the Better regulation strategy may open new perspectives of evolution for the courts in their unique roles as ultimate reviewers (III).

Finally, the Draft Regulation on Data Protection[3] and Draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, prosecu-

---

1 Office of the Privacy Commissioner of Canada, "A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century. A Reference Document From the Office of the Privacy Commissioner of Canada", November 2010, online: <http://www.priv.gc.ca/information/pub/gd_sec_201011_e.cfm>.

2 *R.* v. *Oakes*, [1986] 1 R.C.S. 103.

3 COM(2012) 11 final. A first version of the draft has circulated, dated from 29/11/2011. The final draft introduces certain minor modifications

tion, detection or prosecution of criminal offences or the execution of criminal penalties[4] is still in discussion, but when it is adopted,[5] according to the provisions, data protection impact assessment will become mandatory.[6] So our reflections might be of some help in that context.

I. A DECADE OF BETTER LAW MAKING STRATEGY IN THE EU AND THE SYSTEMATISATION OF IMPACT ASSESSMENTS

In the last decade, interest in improving regulation at the EU level under the pressure of member states has undergone major evolution.[7] The 2001 white paper on European governance set the objective to improve policy-making at EU level in order to respond to the widespread opinion of the population regarding the democratic deficit of the EU.[8] The "better lawmaking" strategy of 2002,[9] one of the core objectives of the "European governance" policy, is organized on six major pillars, which include the necessity to conduct integrated impact assessments in certain policy fields and to consult relevant stakeholders. Transparency and multistakeholders' discussion of this previous impact assessment work is an important instrument for promoting democratic debate since it fosters openness

4 COM(2012) 10 final. The two texts (Regulation and Directive) have been presented by the European Commission DG Justice as complementary. This means that the Regulation is not applicable to the processing activities related to these purposes and subject to this specific directive. This decision seems in contradiction with the suppression of the traditional pillars and might create certain uncertainties as regards the precise scope of the two texts.

5 On this Draft regulation, see Luiz Costa & Yves Poullet, "Privacy and the Regulation of 2012" (2012) 28-3 Computer L. & Sec. R. 254, and Claire Gayrel & Romain Robert, "Le projet de règlement en matière de protection des données: premiers commentaires" (2012) 190 *Journal de Droit Européen* 173.

6 The obligation to conduct Data Protection Impact Assessment as a third principle, is established by Article 33§1 of the draft Regulation and Article 31 of the draft Directive

7 Laurent Vogel & Eric Van Den Abeele, *Better Regulation: Perspectives critiques*, Report 113 of the European Trade Union Institute (ETUI, 2010).

8 White Paper on "European Governance" of 25 July 2001, COM (2001) 428 final.

9 Communication from the Commission "Governance Strategy, Better lawmaking of 6 June 2002, COM(2002)275 final.

with regard to decision-making processes. Impact assessment is a procedure by which one distinguishes non-plausible from plausible risks, and ranks the possibility that the latter will occur.

The adoption of an inter-institutional agreement on "better lawmaking"[10] requiring the conduct of systematic impact assessments prior to every major legislative action,[11] and the subsequent establishment of the Impact Assessment Board in 2006 shows how the practice of impact assessments has been rapidly integrated in the EU legislative process. Conceived as an *aid to help* the institutions to reach properly considered decisions, the objective of which is to strengthen evidence-based lawmaking, it would in any case be destined to substitute political decisions.[12] Impact Assessment Guidelines were adopted in 2005 and subsequently modified in 2009.[13] They provide the methodology to apply in conducting IAs, which traditionally focus on economic, social and environmental impacts of envisaged legislative options. Following a series of criticisms, the Directorate General Employment has enacted specific accompanying "Guidelines and Equal Opportunities with respect of the assessment of social impacts" in order to improve the quality and reliability of IAs in this respect.

Fundamental rights were however not originally perceived as requiring specific attention. This explains why impact assessments of security measures entailing interference with privacy and data protection rights have not focused on the privacy issues raised, but have been dealt with taking into account various criteria, including subsidiary and proportionality tests, economic costs tests for industry and/or member states, internal market tests, and competition tests, which are at the origin of the

10 On this inter-institutional Agreement, read Yves Poullet, "Technologies de l'information et 'co-régulation': une nouvelle approche", in *Liber Amicorum M. Coipel* (Antwerpen: Kluwer, 2004) 167; Yves Poullet, «Mieux légiférer, la corégulation et l'autorégulation dans la politique législative européenne», (2007) 142 *Journal des Tribunaux-Droit Européen.*

11 European Parliament, Commission, Council Inter-institutional Agreement on better lawmaking, OJEU C 321/1, 31/12/2003, points 25 to 30.

12 Inter-institutional Common Approach to Impact Assessment (IA), point 6.

13 Impact Assessment Guidelines of 15 January 2009, SEC(2009)92.

systematisation of IAs: making the "better lawmaking" agenda contribute to the Lisbon strategy objective to improve European competitiveness.

The concern for addressing specific attention to fundamental rights issues in any legislative action has recently been established through the adoption of two documents written by important commissions. First, the Commission communication on "Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union" provides that any legislative proposal having an impact on fundamental rights must include specific explanations of how the proposal complies with the Charter,[14] implying that: "the use of a standardised recital merely noting conformity with the Charter is to be avoided".[15] In order to improve the examination of legal validity of legislative proposals, these are required to answer to a new "Fundamental Rights Checklist":

> 1. What fundamental rights are affected?; 2. Are the rights in question absolute rights (which may not be subject to limitations [...]; 3. What is the impact of the various policy options under consideration on fundamental rights [...]?; 4. Do the options have both a beneficial and negative impact, depending on the fundamental rights concerned [...]?; 5. Would any limitation of fundamental rights be formulated in a clear and predictable manner?; 6. Would any limitation: a) be necessary to achieve an objective of general interest or to protect the rights and freedoms of others? Be proportionate to the desired aim? Preserve the essence of the fundamental rights concerned?[16]

Second, the assessment of legislative proposals' impacts on fundamental rights has, like the guidance provided by the DG Employment with respect of social impacts, recently been strengthened with the adoption of specific Operational Guidelines on the 6th of May 2011.[17] At that time, no legislative proposal with an IA following these specific guidelines had yet been adopted.

Very recently, on January 25th 2012, the European Commission presented its proposal for a regulation on the protection of individuals with regards to the processing of personal data and on the free movement of such data, the so-called "General Data Protection Regulation",[18] in order to modify the current European Data Protection regime under the Directive 95/46. This draft regulation aims at imposing the obligation to conduct data protection impact assessment[19] according to article 33: "[w]here processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes [...]". Having taken into account the data subjects' views, as discovered by following §4 of Article 33, industry and governments have to evaluate risks not only as specified in Article 33§2 on data protection but more broadly with respect to the different liberties as mentioned in the Article 33§3 and with respect to the human dignity of the data subjects in order to justify their decisions.

Beyond verification of legal compliance, Privacy Impact Assessments (PIAs) "have to consider privacy risks in a wider framework that takes into account the broader set of community values and expectations about privacy".[20] Consequently, PIAs are related to a kind of political legitimacy of decisions concerning privacy and data protection. What balance will data protection impact assessment (DPIA) reach with regards to

14 Communication from the Commission "Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union" of 19 October 2010, COM(2010)573/4.

15 *Ibid.* at 7.

16 *Ibid.* at 5.

17 Commission Staff Working Paper on "Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments" of 6 May 2011, SEC(2011)567 final [Commission Staff Working Paper].

18 COM(2012) 11 final. A first version of the draft has circulated, dated from 29/11/2011. The final draft introduces certain minor modifications.

19 On "Privacy Impact Assessment", see notably, Roger Clarke, "Privacy impact assessment: Its origins and development" (2009) 25 Computer L. & Sec. R. 123. This article provides two appendices with a list of examples of PIA documents and references to guidelines describing different PIA methodologies.

20 Adam P. Warren et al., "Privacy Impact Assessments: international experience as a basis for UK guidance" (2008) 24:3 Computer L. & Sec. R. 235.

"rights and freedoms of data subjects"? Is DPIA a parameter of a general duty of care? If so, how can we determine responsibility and liability for actions according to this parameter?

II. Privacy v. security balancing in EU impact assessments and legislative reviews: building validity of rules

The trend towards developing processes and methodologies, notably through multiplication of decision-making tools such as impact assessments, can be analysed, from a legal theory perspective, as a search for validity for the norms to be enacted. The main concern behind these attempts is indeed to produce valid norms through a legitimating decision-making process. The issue of validity of norms is a continuing concern for legal theorists. With respect to balancing the right to privacy with security interests at the EU level, we have found that the better regulation strategy and its instruments of implementation, such as impact assessments and review studies of legislative measures, encapsulate this essential concern for the validity of norms. As proposed by R. Summers,[21] the validity of a public or private norm would rest on the interaction of three essential criteria: legitimacy, effectiveness and legality.

- The **"legitimacy"** criterion is "source oriented[22] and underlines the question of the authors of a norm. This quality of the norm means that the authorities in charge of the norm must be promulgating given the power to do so by the community or communities of the persons which will have to comply with the rule they have enacted. This legitimacy is obvious as regards traditional state authorities acting in conformity with the competence devoted to them by a constitution. It is less obvious when the regulation is the expression of private actors themselves, as is the case with self-regulation, particularly when certain obscure associations or even private companies are given the power to impose their own technical standards.
- The **"conformity"** criterion is "content oriented" and designates compliance of normative content vis-a-vis fundamental society values, i.e., those embedded undoubtedly in legal texts but also those considered as ethical values to be taken into account by the legal system. Again, this criterion is quite easy to satisfy and to verify in the case of traditional texts issued by governmental authorities, insofar as these texts must be taken in the context of already existing rules with superior values. It seems more intricate to satisfy this criterion when compliance with existing legislative texts is not systematically checked insofar as these texts do not exist or are not clearly identified. Indeed self-regulation is often a way to avoid the traditional, constitutionally foreseen regulatory methods of rule-making.
- Finally, the **"effectiveness"** criterion is "respect oriented". To what extent will a norm be effectively respected by those to whom the norm is addressed? So, awareness of the norm, sanctions and enforcement are central for determining the effectiveness of a norm. This criterion means in particular the fact that addressees of the norm need to be aware of the content of the norm, but also that norms have to entail costs if addresses fail to comply.

On this point, it is quite clear that technology, as Joel Reidenberg[23] has pointed out, self-regulatory mechanisms like code of conduct labelling systems and ODR might provide additional ways for promoting and enforcing normative instruments.[24]

---

21 Robert Summers, "Towards a better general theory of the legal validity" (1985) 16:1 Rechtstheorie 65. Concerning these three criteria applied by the interinstitutional agreement, see Y. Poullet, supra note 10.

22 See, on this distinction between "source-oriented tests", "content oriented tests" and "effectiveness-oriented tests", R. Summers, supra note 21.

23 Joel R. Reidenberg, "Lex Informatica: the Formulation of Information Policy Rules through Technology" (1998) 76 Texas Law Rev. 553. On the same point, see our remarks about the relationship between law and technology in "Technology and Law: From Challenge to Alliance", Festschrift für W. Kilian, forthcoming and definitively Lessig's fundamental reflections in Lawrence Lessig, Code and other Laws of Cyberspace, New York, Basic Books, 1999

24 Notably, Bertrand Du Marais, "Autorégulation, régulation et co-régulation des réseaux", in Georges Chatillon, ed., *Le droit international de l'Internet* (Bruxelles: Bruylant, 2002) 296. On the characteristics of the Internet which justify a self-regu-

We propose to analyse the balancing of the right to privacy and security interests in light of these three criteria.

The cases referred to in the present paper are those embedding privacy v. security balancing and for which an impact assessment *ex ante*, or *ex post* (review process) has been carried out in the last decade. We will look at the case of the so-called Data Retention Directive,[25] which was the object of an impact assessment in 2005 before its controversial adoption in 2006 and recent review in 2011. We will also look at the European proposals for a European Passenger Name Records system, which were the objects of a first impact assessment in 2007 and a second impact assessment in 2011. Because a European terrorist financing tracking program, modelled on the U.S. TFTP should be under study in the next months at the EU level, we will also look at the review of the EU-US Swift Agreement.

First we will look at the criterion of legitimacy according to which the validity of a norm rests in part on the participation of interested parties to its elaboration. Through our case studies, we will see that the consultation of the "relevant stakeholders" by the Commission reveals highly restrictive and questionable (A). Then, we will look at the criterion of effectiveness, which assesses the performance of a norm according to its expected effects, and see the weaknesses of argumentation in this matter, which calls into question the importance of effectiveness as a criterion

latory decentralized approach rather than the traditional top-down approach based on a legislative and nationally bounded approach, see David G. Post & David R. Johnson, *The New Civic Virtue of the Net*, online: <http:// www.stbr.stanford.edu/ STLR/Working_Papers/97_Post1/contents.htm>: "The ideal of national debate among wise elected representatives regarding the overall public good may be replaced, online at least, by a new architecture of governance that allows dispensed and complex interactions among groups of individuals taking unilateral actions and seeking more local goods and solutions. Instead of attempting to rely even upon the best of our democratic traditions to create a single set of laws imposed on the net from the top down [...]."

25 EC, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, [2006] O.J., L105/54 [*Directive 2006/24/EC*].

for validity in security matters (B). Finally, we will focus on the criterion of legality, understood here as consistency of the content of legislation with higher norms, in particular Article 8 of the European Convention for Human Rights. We will show how, in our view, the issue of data protection safeguards in privacy v. security balancing contribute to evacuation of substantial liberties issues (C).

A. Building legitimacy: consultation/participation of "relevant stakeholders"

One of the fundamental objectives of the European governance and "better lawmaking" strategy is to increase the interplay between policy-makers, experts, interested parties[26] and the public at large in the policy-making process. The "dialogue" between the European Commission and these heterogeneous parties in policy-making matters occurs through a wide range of instruments and channels.[27] Two major documents organize the consultation of interested parties and recourse to expertise. The "minimum standards for consultation",[28] applicable to the IA process, provide that consultation may be open to the general public, restricted to a specific category of stakeholders (any member in the selected category can participate) or limited to a set of designated individuals/organisations

26 EU documents refer both to "relevant stakeholders" and "interested parties", without clarifying whether there is any difference between groups. An interested party is understood by the Commission as "an individual or group that is concerned or stands to be affected – directly or indirectly – by the outcome of a policy process; or represents the general interest of groups concerned by the such an outcome, within and outside the EU" COM (2002) 713 final, footnote n° 4.

27 See L. Vogel & E. Van Del Abeele, supra note 7 at 62-70. Among various channels, there are the European Economic and Social Committee, Committee of the Regions institutionalized in the EU treaties, the so-called "comitology" referring to the committee system with representatives of member states, the various technical committees, the external consultants of the Commission and others... The "dialogue" with "civil society" may occur through trade unions institutes, NGOs, the public at large etc.

28 Communication from the Commission "Towards a reinforced culture of consultation and dialogue – General principles and minimum standards of consultation of interested parties by the Commission" of 11 December 2002, COM(2002)704 final

(only those listed by name can participate). Collection of expertise[29] is destined to increase the scientific-evidence based approach of decision-making in view of convincing interested parties that policy-making choices and decisions have duly been assessed.[30] Basically, the European Commission is first required to collect the relevant expertise and data internally, by consulting other DG expertise where needed. Where fundamental rights are at stake, the Fundamental Rights Guidance specifies that civil servants from the DG Justice should be invited to the Impact Assessment Steering Group.[31] Consultation of external experts may also be envisaged. Precisely, it is at the time of carrying out impact assessments that both "interested parties" and "experts" can be called upon to contribute to the policy-making process. Consultation of interested stakeholders is an important criterion aimed at building legitimacy of the policy-making process.

In the impact assessments conducted by the European Commission over the last decade with respect to security measures interfering with the right to privacy, consultation of interested stakeholders has been limited to institutionalized actors and groups. In the case of the data retention IA of 2005, contributions from member state governments, member state police sector, telecommunications industry and Working Party 29 have been solicited.[32] For the preparation of the first PNR IA of 2007, consultation of "all relevant stakeholders" has been solicited through a "questionnaire" sent to all the member states, the data protection authorities of the member states, the European Data Protection Supervisor, and air

29 Communication from the Commission on the collection and use of expertise by the Commission: principles and guidelines, Improving the knowledge base for better policies, of 11 December 2002, COM(2002) 713 final

30 *Ibid.* at 3. See also Alberto Alemano, "Science and EU Risk Regulation: the Role of Experts in Decision-making and Judicial Review", in *European Risk Governance – Its science, its inclusiveness and its effectiveness*, Connex Report Series n° 6, Vos ed., February 2008

31 Commission Staff Working Paper supra note 17 at 11.

32 *Extended Impact Assessment of 21 September 2005 annexed to the Proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services and amending directive 2002/58/EC*, SEC(2005)1131 at 23-24.

transport and air carriers associations (Association of European Airlines, Air Transport Association of America, International Air Carrier Association, European Regions Airline Association, International Air Transport Association).[33] The new PNR IA of 2011 did not reopen consultation. It is supposed to be based on the consultations carried out in 2007, but also on the various opinions expressed by industry, data protection authorities and the Fundamental Rights Agency[34] on the European proposal for a PNR system, and on the opinions expressed with respect to the US, Canadian and Australian PNR systems.[35]

Participation and consultation of civil society at large has not been carried out in the framework of such proposals. Privacy and civil liberties interests have quasi-exclusively been represented by data protection authorities (except in the case of the first PNR proposal which was the object of an opinion from the Fundamental Rights Agency, which is said to be taken into account in the second PNR proposal). It is therefore implied that data protection authorities are the legitimate *relevant stakeholder* to provide consultation to the EC when a measure involving privacy/security balancing is at stake. This identification of "interested stakeholders" is in our view, questionable. As we will stress further, it contributes to reducing concerns for fundamental rights protection to the issue of data protection safeguards. Though DPAs are unavoidable consultant and advisory parties, the fact that they may be the only civil liberties representatives consulted is definitely restrictive. Possible changes might come with future application of the specific Operational Guidance for Fundamental rights in impact assessments where it is recognized that:

33 *Impact Assessment of 6 November 2007 accompanying the proposal for a framework decision on the use of Passenger Name Records (PNR) for law enforcement purposes*, SEC(2007) 1453, I.2 and I.3.

34 Opinion of the Fundamental Rights Agency of 28 October 2008 on the proposal for a Council Framework decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, online: <www.fra.europa.eu>.

35 *Impact Assessment of 2 February 2011 accompanying the proposal for a directive on the use of Passenger Name Records data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes*, SEC(2011)132 final, I.2.

there are a number of stakeholders working in the field of fundamental rights that can provide valuable input during the consultation phase, such as non-governmental organizations specialising in human rights, health, development, environmental and social issues more generally.[36]

Consultation and contributions from civil liberties associations definitively would be valuable and extend the range of actors participating to the law-making process.

B. Building effectiveness

While effectiveness cannot replace necessity, it however constitutes one of the underlying conditions of the proportionality principle for assessment of any invasion of privacy in compliance with Article 8 of the European Convention for Human Rights. Effectiveness, as one of the central pivots of legal validity, refers to the performance of the norm, its aptitude to reach its core objectives.[37] Law is increasingly submitted to the test of effectiveness, which also contributes in turn to build its legitimacy. The recourse to experts discussed above must also be analysed in this context, where such experts are invited to participate to the legislative process and/or review process of a norm in order to assert its performance with respect to the objectives assigned to it.

Here, we will define effectiveness as whether there is evidence that the intended security policy will produce the expected effects (at the pre-legislative stage, such as at the time of impact assessment) or whether it has indeed produced the expected effects (at the time of review). We will see that a fundamental Commission and member state concern seems to build the legitimacy of the measures on rational indicators. At the same time, the way in which necessity and effectiveness of the measures are justified and assessed proves to be rather a structured political discourse

[36] Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, at 13

[37] François Ost & Michel Van de Kervoche, "De la pyramide au réseau ? Vers un nouveau mode de production du droit ? " (2000) 44 Revue interdisciplinaire d'études juridiques 329.

than a scientific-based evidence approach, in spite of the EU's own policy-making requirements described earlier.

Here, we come back to how the issue of effectiveness is dealt with in the case of the data retention directive, the processing of PNR data and the transfer of financial data towards the US for the purposes of the US Terrorist Finance Tracking Program.

1. Data retention effectiveness: a structured political discourse

The retention of traffic and location data for law enforcement purposes probably constitutes the most controversial example of EU legislative action violating privacy, in particular from the perspective of its asserted effectiveness.

For the record, a core objective of the Data Retention Directive proposal was harmonisation of national legislations to avoid distortions in competition in the internal market, since five member states started to introduce retention obligations at the national level. This objective has been advanced to defend the adoption of a Directive instead of a Framework Decision under the former third pillar.[38] The "do nothing option" was therefore discarded by the Commission on the grounds that the risks of internal market distortions would "in all likelihood continue to increase" if other member states adopted similar measures.[39] The necessity to retain traffic data for law enforcement purposes has been asserted mainly on the basis of anecdotal evidence that such a measure would meet the needs of law enforcement authorities. In particular, the "data preservation" option, a system of targeted collection of traffic data that would assist specific criminal investigations, supported by industry and data protection authorities was discarded by the Commission in favour of the data retention option, involving the indiscriminate, blanket retention of traffic and location data of all subscribers on the grounds of

[38] *EUCJ, Ireland v. European Parliament and Council*, C-301/06, [2009] ECR I-00593.

[39] Impact Assessment annexed to the proposal for a directive on data retention, supra note 32 at 9.

its presumed greater effectiveness for the purposes of crime investigations.

While poor objective data were supplied to support the effectiveness of the proposal in 2005, the evaluation report expected five years after the entrance into force of the Directive[40] was even more crucial for confirming the ambitions of the instrument. However, the 2011 evaluation report[41] found that the effectiveness of the data retention Directive definitely-turns to be a politically based discourse.[42] First, with respect to the objective of harmonisation of national legislation in the matter of data retention, the Directive clearly failed. It can even be asserted that implementation of the Directive in member states has proven to be "counter-productive", creating a far more disjointed situation than had previously existed between member states, leading European Digital Rights to question whether the Directive itself would constitute an obstacle to free movement of electronic communications services.[43] In spite of this result, the Commission still supports a revision of the Directive, rather than its abandonment. Second, with respect to the law enforcement objectives, the Commission evaluation appears to have been carried out with the aim to reach the conclusion that the Directive produced the expected effects. Benefits to criminal investigations are reported through general statistics provided by some of the member states – where these were available – and with anecdotal examples of criminal cases. As underlined by European Digital Rights (EDRi), the evaluation report of the Commission therefore produce very limited results and notably fails to demonstrate

40 *Directive 2006/24/EC*, supra note 25 at art. 14.

41 *Evaluation Report of the data retention Directive (Directive 2006/24/EC) from the Commission to the Council and the European Parliament of 18 April 2011*, COM(2011)225 final.

42 European Digital Rights "Shadow evaluation report on the Data Retention Directive (2006/24/EC)" of 17 April 2011, online: <http://www.edri.org/files/shadow_drd_report_110417.pdf>.

43 *Ibid.* at 5.

the added value of the data retention option instead of the preservation data option for the purpose of criminal clearance.[44]

2. The processing of PNR and financial data: effectiveness widely "under cover"

The famous forerunner in processing PNR and financial data for law enforcement purposes, in particular the fight against terrorism and other organized crime activities, is the United States, which first introduced security programs requiring the transfer of these data from other countries, including European member states. EU-US agreements have been concluded in this matter, at various rates, according to the sensitiveness of the issues.[45] While it is not the object of this paper to go back over the ongoing history and grounds of EU-US cooperation in transfers of information in the criminal field ongoing,[46] the "import" of both tools, i.e. processing of PNR data and financial data, are being studied in the EU. The effectiveness of the US experiences in this matter would therefore be supposed and expected to provide conclusive arguments for the EU to adopt converging actions. However, in both cases, the lack of publicly available data, whether on secrecy grounds or because they simply do not exist, does not allow outside commentators or the public at large to appreciate the necessity of the measures, and therefore leaves the issue of the effectiveness of such processing widely "under cover".

Indeed, the Report on the joint review of the implementation of the Agreement between the European Union and the United States of

44 *Ibid.* at 7. See also the *Report of the Scientific Services of the German Parliament*, Report WD7-3000-036/11, online: <http://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.docx>.

45 In this field the EU-US cooperation has evolved from scandals (ECHELON, SWIFT) to negotiations (adoption of the so-called PNR and SWIFT agreements for example) under a more or less constraining US foreign affairs policy.

46 For a retrospective and overview of EU (and member states) – US cooperation in criminal matters, see Els De Busser, *Data Protection in EU-US Cooperation, A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities* (Antwerpen: Maklu, 2009).

America on the processing and transfer of Passenger Name Records provides little, if no, evidence that PNR serves the purpose of supporting the fight against terrorism and serious crimes. In this respect, the report mentions only that "the EU team has been satisfied that this is indeed the case".[47] Data are simply not made publicly available. While the European Commission presented its proposal and accompanying impact assessment for a framework decision establishing a European PNR system seven months after the conclusion of the EU-US PNR Agreement in 2007, no mention was made in this document of the US PNR system or similar ones established elsewhere. This can be explained only by the Commission's will to avoid associating the European proposal with the US system in order to reduce possible challenges at the internal level. Scholars nevertheless did not fail to note the surprising similarity between the Commission's proposal and the EU-US Agreemen.[48]

The review of the transfers of financial data from the Belgian financial society SWIFT to the US for the purposes of the US Terrorist Finance Tracking Program (TFTP) is at the very least enigmatic regarding the effectiveness of the US program. While the EU joint review team asserts the "operational value" for the FBI, but also insists on the "unique value" of the program, which is described as "the most important Agreement the US has in place in this area",[49] it specifies that it would be premature to address the issue of the effectiveness of the program. If previous reports (notably those delivered by the French anti-terrorist Judge Jean Louis Bruguière prior to the adoption of the Swift agreement) strongly insisted on the effectiveness of the program and therefore its value for the EU,

47 *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Records (PNR) data by air carriers to the United States Department of Homeland Security (DHS)* (Brussels: 2010) at 4.

48 Pabryk Pawlack, "Made in the USA? The influence of the US on the EU's Data Protection Regime, the PNR example" 2009, Centre for European Policy Studies.

49 *Report of 31 march 2011 on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program 17-18 February 2011*, SEC(2011) 438 final (Brussels: 2011) at 8.

one remains circumspect about the conclusions of the review team, which seems satisfied with "'indirect indications'" of the added value of the TFTP derived information to counter-terrorism investigations".[50] The caution with which the drafters of the report evoked the effectiveness of the program has probably contributed to the European Commission's delay in presenting a European TFTP proposal as initially expected in August 2011.

3. Effectiveness: a criterion for validity of rules?

The examples quoted above raise the question of to what extent effectiveness of security measures that violate privacy can still be considered as a criterion for their validity in "democratic society". In the matter of security and law enforcement at large, any failure has become inadmissible, and leads to questioning of the existing security apparatus. The case of air transportation and airport security is telling.[51] It appears that whether there is no evidence of effectiveness, or whether the only evidence of effects is anecdotal and the effects are not those anticipated, there are still no accepted reasons to oppose the adoption of a measure or to question it. A major issue remains with respect to secrecy. Since concerning security, secrecy as a necessary element for effectiveness can be put forward to prevent disclosure of data and potential challenges or debates concerning these data, it is difficult for outsider commentators or the public to assess the effectiveness of a given measure or to potentially question the necessity of a measure violating privacy.

Another point is suggested by the comparison with the Canadian approach. The Canadian DP report underlines the importance of not only addressing the question of the added value of the measures taken but also of being sure that the design and organisational measures will guarantee future respect of the balance. In other words effectiveness also means "embedding privacy in the information management" and "calibrating

50 *Ibid.* at 9.

51 See for example the case of the failed terrorist attempt of Christmas 2009, in which a Nigerian attempted to get on a plane with liquid explosives and the subsequent introduction of body scanning in European airports.

the system": Are there management procedures that guarantee that the chosen balance will be respected effectively? The answer to the question requires a systematic analysis of the accountability procedure and the way to ensure the transparency of the decision taken. The effectiveness of the means of individual access, a complaint procedure and other sufficient security safeguards embedded in the design of the information system[52] have to be implemented in order to guarantee this balance.

C. Building legality: when data protection safeguards supplant debate on freedom

1. The proportionality analysis in EU impact assessments

Violation of privacy by European public authorities is submitted to the well-known proportionality principle, as enshrined in Article 8 of the ECHR and interpreted by the European Court. In the EU system, the principle of proportionality as an unwritten, general principle of law governs law-making and adjudication in virtually all domains of European law, notably with respect to the internal market policy (free movement of goods, persons, capital, services and establishment). Expressly established in Article 5§1 of the Treaty on the EU,[53] the principle of proportionality governs the exercise of EU competences, along with the subsidiary principle. Conceived as an instrument for the delimitation of

52 This necessity refers to the principle "Data protection by design". Quite interesting is the fact that the Draft Regulation on Data Protection imposes this principle which is defined in the following terms: "Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject" (art. 23.1). As asserted by Anne Cavoukian, DPA Commissioner from Ontario, Canada in the introductory remarks to the Privacy Guidelines for RFID Information Systems, online: <http://www.ipc.on.ca>: "Privacy and Security must be built in from the outset – at the design stage".

53 Article 5§1 of the *Treaty on the European Union* (ex art. 5§3 of the *Treaty of the European Community*).

competences between the Union and its member states, the principle of proportionality nevertheless shares common functions with the principle of proportionality as applied by courts in human rights adjudication. In both cases, proportionality analysis implies verification of justification for the legitimacy of the measure, its suitability, its necessity via the well known least restrictive means test, and final balancing *stricto sensu*. In the EU, the legitimacy, suitability and least-restrictive means tests of a measure appear to be equally justified with respect to the very content of the measure, so legislative intervention occurs at the EU level rather than at the member states level.

Though impact assessment does not aim at providing the legal arguments asserting compliance or non-compliance with the European treaties or the European Charter of Fundamental Rights,[54] a task which is assigned to the European Commission at the time of preparing an advanced draft proposal, it is recognized that legislative tools, and in particular impact assessment, contribute to carrying out constitutional tasks.[55] Where fundamental rights are at stake, in particular privacy and data protection rights, the proportionality analysis carried out in the impact assessment affords the basis for the justification of the necessity of the measure, whether to respect of the least-restrictive means test, or the proportionality *stricto sensu* test. In this framework, proportionality analysis in EU impact assessments conducted during the last decade in the matter of privacy v. security provides an interesting opportunity for constitutional interpretation of privacy v. security balancing in the EU. This also supports the view that impact assessments can be a catalyst for

54 Or with the *Council of Europe Convention on Human Rights* and its interpretation by the Strasbourg Court. As regards the relationship between the *EU Charter and the Council of Europe Convention*, see the Commission Staff Working Paper, supra note 17: "The Charter explicitly provides that in the cases where the rights proclaimed by the Charter are the same than those enacted by the Convention, the meaning and scope of these rights must be the same as those laid down by the ECHR and the Strasbourg Court."

55 Anne Claartje Margret Meuwese, *Impact Assessment in EU Lawmaking* (Austin: Kluwer, 2008).

legal principles, and have the potential to afford a new mode of operationalization of proportionality.[56]

In the case of the data retention Directive, probably the worst reasoning supporting the proportionality of an EU action can be reduced to a formal statement that the proposal *is* proportionate. As already mentioned, no serious data have been produced concerning the various options in the data retention IA capable of showing that there were no less intrusive means – for example, with respect to the data preservation option – to achieve the policy objectives.

The impact assessment relating to the proposal for the adoption of a framework decision establishing a European PNR system shows some improvements from a strict methodological point of view, addressing various options in a more extensive way. However, the IA does not deal expressly with the requirements of proportionality and subsidiary. The "EU right to act" is asserted here again on the grounds of risks of distortion of the internal market and threats of terrorist and organized crime. When addressing the issue of fundamental rights, the PNR proposal is positioned foremost as an instrument destined to "ensure the right of the European citizens to enjoy all their fundamental rights, and especially the right to life and physical integrity".[57] It is only recognized that the processing and exchange of PNR data "might interfere with the right to the protection of private and family life and to the protection of personal data". The proportionality of the measure with respect of travellers' right to privacy and data protection is ultimately dealt with at the time of comparing decentralized and centralized collections of data, the decentralized option being considered to be "more likely for such interference to be deemed proportionate".

The proposal for a Directive establishing a European PNR system and the new impact assessment accompanying the proposal published in February 2011 is a first illustration of the renewed political framework for deliberations as proposed in the recommendations of the European Commission in the same semester. It shows substantive improvements

[56] *Ibid.* at 58-60.

[57] *Impact Assessment PNR Proposal*, supra note 35 at 13.

compared with the 2007 one, and they have also been recognized by the EDPS.[58] The impacts on fundamental rights are said to "have been assessed in line with the Fundamental Rights checklist as provided for in the Commission's strategy for the effective implementation of the charter."

The IA considers that the PNR proposal may interfere with the right to protection of private life and protection of personal data. Considering that these rights can both be subject to limitations under specific conditions, the IA seeks to adopt the most reasonable option, and recalls the fundamental data protection principles applicable to the said proposal. The last question of the fundamental checklist as to whether "the essence of the fundamental right" is preserved is however left unanswered.

2. How data protection safeguards eliminate debate on freedoms in IAs

In our view, identification of fundamental rights issues in IAs proves to be restrictive. In the data retention IA, the fundamental right of non-suspected citizens to secrecy of communications, i.e., the right to communicate freely and outside the scope of surveillance of public authorities for people who are not involved in a criminal investigation, is never expressly discussed. While a general statement recognizes the "privacy" interference of the measure, data protection guarantees are more extensively discussed: what are the purposes for which retention is required? How long do data need to be kept to achieve these purposes? Which kind of data? The same can be observed in both PNR IAs. In particular, though the PNR IA carried out in 2011 should have submitted the PNR proposal to the new "fundamental rights checklist", the IA proves unsatisfactory in this respect. As underlined by the Fundamental Rights Agency, the Commission IA acknowledges only that the use of PNR data interferes with the fundamental rights of protection of privacy and protection of personal data, leaving unaddressed other fundamental rights possible

[58] Opinion of the EDPS of 25 March 2011 on the use of PNR for law enforcement purposes at para. 6.

concerned, in particular the right to non-discrimination.[59] As mentioned earlier, the approach consisting in consulting the EDPS and the article 29 Working Party as legitimate guarantors of fundamental rights and civil liberties leads the IA to be focused predominantly on the right to data protection, and contributes to evacuating other fundamental rights concerns from the IA process.

This leads us to wonder whether data protection guarantees could contribute to replacing fundamental liberties debate. Again, the IA does not mention the right to move and travel freely outside the scope of surveillance by public authorities in spite of the critics of the EDPS, who "questioned whether the necessity and proportionality of the proposal had been demonstrated since the proposal concerned a very wide collection of data of innocent people", proposal that contributes to creating a "surveillance society". The balance is immediately shifted to the issue of data protection guarantees and is actually established between the centralized and decentralized options of PNR data collection. This raises the broader question of an evolving complicity between data protection rules and security/surveillance measures. Data protection rules in themselves increasingly appear to provide for the step-by-step method to reach a "privacy compliant proposal" in the Impact Assessments of the European Commission. In the same time, they seem to contribute to removing substantial debate about interferences with other fundamental rights. Conscientious implementation of the "Fundamental Rights Operational Guidance" during the IA process and its checklist must be strengthened and seriously addressed to contribute to a constructive debate instead of affording a tool to avoid substantial fundamental rights assessment.

That reflection leads to a more fundamental concern. In the new EU approach, Data Protection is viewed more and more as a separate constitutional right distinct from privacy. By distinguishing in Articles 7 and 8, Privacy (art. 7) and Data Protection (art. 8) the EU Charter on fundamental rights has already introduced this distinction, but the Draft Data

59 *Opinion 1/2011 of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes, (COM(2011)32 final)* (Vienna: 2011), online: <www.fra.europa.eu>.

Protection Regulation clearly emphasises this dissociation from data protection: the word privacy is gone. Besides, the distinction is reinforced when the Regulation establishes the concepts of "data protection assessment" and "data protection by design", which are clearly unusual terms in comparison with "privacy impact assessment" and "privacy by design". In addition, while the word 'Privacy' appeared 13 times in Directive 95/46, the word is mentioned only three times in the draft regulation. Would be data protection be with its origins? If so, what will be the outcome of this movement? Will new legal correlations between privacy and data protection be established? The outcome of this change are still unknown, but it is certain that affirming the autonomy of the right to protection of personal data does not imply denying privacy as its foundation. That distinction puts protection of liberties at risk since it cuts the data protection regulation from the innovative and quite protective Strasbourg Court's jurisprudence, which repeats that privacy might be considered as the way for achieving the right to self-determination and dignity and, to that extent, might be considered as the condition for all liberties. It must be reasserted that there is an intrinsic link between privacy and data protection legislation conceived as a simple "procedural law' at the service of substantive rights such as privacy.[60] The latter is viewed as a simple tool in an information society for ensuring the various human freedoms and not to be considered as an end *per se*.

III. The European Union Court of Justice and better regulation requirements

The development of the "better regulation" strategy and its implementation tools, among which the impact assessment, raise some questions concerning its enforcement, and in particular their potential judicial review by the European Union Court of Justice. Some scholars predict litigation scenarios that might lead courts to look at whether "better regu-

60 On that point, see Antoinette Rouvroy & Yves Poullet, "The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy", in Serge Gutwirth et al., *Reinventing Data Protection* (London: Springer, 2009) 45 at 56.

lation" requirements have been complied with at the drafting stage of a regulation. Alemanno identified, among other scenarios, the perspective that courts called upon to review the lawfulness of a European act, either within the context of a cancellation procedure or reference for a preliminary ruling procedure, may be led to look at respect of better regulation requirements and compliance with them in order to ascertain whether certain alleged grounds, such as the subsidiary principle or principle of proportionality were well founded.[61] According to Alemanno:

> Although the Court has been able to assess the compliance with the abovementioned principles by Community acts without necessitating any previous evaluation made at the drafting stage of the examined acts, the current practice of carrying out an IA of all major Commission initiatives may lead the Court to refer to such previous evaluations in order to adopt a certain judicial conclusion.

With respect to the review of the principle of proportionality of a privacy v. security balancing of a given measure, the court's own proportionality review conclusions might increasingly rely on pre-legislative proportionality analysis, according "more deference to legislative choices, over time, to the extent that lawmakers demonstrate that they are taking seriously proportionality requirements when they legislate".[62]

Respect of the proportionality principle of any violation of privacy may lead judicial review to slightly, but surely, shift to the issue of whether the European legislator complied with the "better regulation" requirements prior to adoption of the regulation, rather than, focusing on the legality of the content of the measure. Though no judicial review as such can be exercised over the better regulation requirements and compliance with them in a given legislative action due to their non-binding character, recent EUC's caselaw provides an illustration of this possible

61 Alberto Alemanno, "The Better Regulation Initiative at the Judicial Gate: A Trojan Horse within the Commission's walls", paper presented at the *The Evolution of the European Courts: Institutional Change and Continuity 6th International Workshop for Young Scholars*, 2007.

62 Alec Stone Sweet & Jud Matthews, "Proportionality, Balancing and Global Constitutionalism" (2008) 47 Columbia Journal of Transnational Law 73 at 163.

shift.[63] In that case, the E.U. Luxemburg Court declared unvalid provisions of a regulation obliging member states to make publicly available the names of recipients of EU agricultural subsidies as regards natural persons. The Court considered that the measure disproportionally interfered with the right to privacy and data protection. The Court's decision rested mainly on the fact that the Council and the Commission had failed to ascertain, *ahead of adopting the contested regulation*, whether the chosen measure did not go beyond what was necessary for achieving the legitimate policy objective of increasing transparency in management of EU agricultural funds.[64] This caselaw also appears to be at the origin of the adoption of the "Fundamental Rights Guidance", showing the concern of the European Commission to strengthen the argumentation of legislative initiatives to avoid risks of litigation.[65]

In view of the weaknesses and lacunas in implementation of the "better regulation" strategy described in this paper concerning fundamental rights, increasing deference of courts to measures that would have satisfied certain deliberation requirements does not seem desirable to us. Neither respect of regulation tools nor the words of experts in current European impact assessments seem sufficiently valid to supplant judicial scrutiny of fundamental rights compliance at the time of review, since the judiciary is the ultimate guardian of fundamental rights.

Conclusions

Is the European approach an adequate way for achieving the right balance between security and liberties? We remain dubious. We take quite a positive view vis-à-vis the increasing concern of EU authorities for assessing from an earlier stage the impact of any EU legislative proposal concerning fundamental liberties by imposing a human liberties impact assessment and by so creating the conditions for a real dialogue among all stakeholders as regards this debate. But in the same time, we

63 *Schecke and Eifert*, joined cases C-92/09 and C-93/09, [2010] ECR I-0000.

64 *Ibid.* at 81-83

65 "Operation Guidance in taking into account fundamental Rights in Commission impact assessments", *ibid.* at 4.

have to denounce the fact that until now the outcomes of these debate in the different cases analysed have been quite disappointing and reveal a quite limited superficial analysis. Moreover, we have seen that this debates has been reduced to a simple comparison between the interests at stake without taking into consideration the question of the present and future effectiveness of the proposed legislation and, overall, in sufficient analysis of their impacts on our different fundamental liberties and human dignity. In our opinion, this trend will be exacerbated when we consider the reduction of the privacy debates to data protection issue. This entails forgetting the roots of data protection legislation, as demonstrated by our considerations about the drafted data protection package still in discussion.

Another reason justifying our concern is our authorities' unsufficient reflection on the role of experts in shaping the functioning of our information society. There is a risk that both our legislative authorities and our Courts will lose their fundamental roles owing to excessive confidence in such preliminary expertise. If this were to happen, our democracy would be at risk.